

# A nova Lei Geral de Proteção de Dados Pessoais

Principais repercussões para a atividade empresarial

Parte I

---

**Ana Frazão**

Advogada. Professora de Direito Civil e Comercial da UnB. Ex-Conselheira do CADE.

---

Como procurei demonstrar em artigos anteriores, são muitas as inquietações que a economia movida a dados vem gerando sobre os direitos dos usuários. Afinal, os dados pessoais, muitas vezes coletados de forma ilícita, sem a ciência e a autorização informada dos titulares, estão se tornando os novos insumos da nova economia, o que pode comprometer não apenas a privacidade dos usuários, mas também a identidade pessoal, a autodeterminação informativa, a liberdade, as oportunidades e perspectivas do presente e do futuro das pessoas e a própria democracia<sup>1</sup>.

É nesse contexto que precisa ser compreendida a recente Lei nº 13.709/2018, que trata da proteção de dados no Brasil, com muitas semelhanças em relação à regulação europeia. Apesar de algumas limitações do seu texto, bem como do veto presidencial quanto à autoridade responsável pela fiscalização e monitoramento – questão que supostamente será resolvida por superveniente medida provisória ou projeto de lei -, não há dúvidas que a lei trouxe importantes avanços, os quais implicarão significativas modificações para a atividade empresarial e para toda a sociedade.

---

<sup>1</sup> Para maiores informações, ver, dentre outros, FRAZÃO, Ana. *Data-driven economy e seus impactos sobre os direitos de personalidade: indo além da privacidade e do controle aos dados pessoais*. <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-mercado/data-driven-economy-e-seus-impactos-sobre-os-direitos-de-personalidade>. Coluna de 18.07.2018.

O objetivo da presente série de artigos é precisamente refletir sobre as principais alterações que a nova Lei Geral de Proteção de Dados traz para a atividade empresarial. Afinal, apesar da *vacatio legis* de 18 meses, estima-se que a total adaptação das empresas não será tarefa fácil, assim como não será simples resolver todos os problemas interpretativos que decorrem da lei.

Passando para o exame do texto da lei, a primeira observação importante é que fica claro que o regime de proteção de dados não tem por finalidade apenas a de tutelar a privacidade dos usuários. A própria lei menciona, logo em seu art. 1º, que o seu objetivo diz respeito a proteger "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural."

Em seguida, a lei disciplina, em seu art. 2º, os seus fundamentos, os quais são, além da privacidade, a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa; a livre concorrência e a defesa do consumidor; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas pessoas naturais.

Ao se referir expressamente ao livre desenvolvimento da personalidade, à cidadania e à dignidade, a lei certamente procura evitar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais, os quais, processados por algoritmos, são capazes de fazer diagnósticos e classificações dos usuários que, por sua vez, podem ser utilizados para limitar suas possibilidades de vida. Mais do que isso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive o político.

Como uma forma de reação a tais utilizações indevidas, a Lei Geral de Proteção de Dados deixa claro que pretende proteger o usuário-cidadão plenamente, em todos os aspectos da sua autonomia pública e privada, valorizando e preservando sua autodeterminação informativa e sua capacidade decisória. Trata-se, portanto, de eixo valorativo em torno do qual devem ser compreendidas e interpretadas todas as demais disposições previstas pela lei.

Apresentados os objetivos e os fundamentos da proteção de dados, é importante explorar alguns dos conceitos-chave utilizados pela lei, tais como o de dados e o de tratamento de dados. No que diz respeito ao primeiro, a lei define dado pessoal como "informação relacionada a pessoa natural identificada ou identificável" (art. 5º, I). Apresenta igualmente a definição de dado pessoal sensível como o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (art. 5º, II).

O titular dos dados, que é o sujeito protegido pela lei, é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (art. 5º, V), motivo pelo qual as pessoas jurídicas ficaram de fora do seu escopo de tutela. Acresce que, como se verá ao longo da série de artigos, a categoria dos dados pessoais sensíveis terá repercussão no regramento jurídico destes, diante da sua importância e do maior potencial lesivo decorrente da sua indevida utilização.

Outro conceito-chave para a compreensão da lei é o de tratamento de dados, que foi definido como "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração" (art. 5º, X).

Como se pode observar, o conceito de tratamento de dados é extremamente amplo, o que ajuda a entender que a lei, tal como previsto no seu art. 3º, aplica-se a qualquer operação de tratamento de dados realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada em território nacional ou em casos em que os dados pessoais forem coletados no Brasil, digam respeito a indivíduos localizados em território nacional ou o tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços no Brasil.

Verdade seja dita que, nos termos do art. 4º, são exceções à aplicação da lei o tratamento de dados (i) realizado por pessoas naturais para finalidades exclusivamente particulares e não econômicas, (ii) realizado para fins exclusivamente jornalísticos, artísticos e acadêmicos, aplicando-se a estes últimos os arts. 7º e 11 da lei, (iii) realizado para fins exclusivos de segurança pública, defesa nacional, segurança do Estado, e atividades de investigação e repressão de infrações penais e (iv) provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

A parte inicial da Lei Geral de Proteção de Dados contém igualmente os princípios que devem orientar o tratamento de dados. Trata-se de parte importantíssima da nova lei, uma vez que tais princípios auxiliarão a compreensão de muitas das regras que serão examinadas posteriormente.

Nos termos do art. 6º, os princípios do tratamento de dados no Brasil são, além da boa-fé objetiva, os seguintes:

(i) **princípio da finalidade**, descrito como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (inciso I);

(ii) **princípio da adequação**, descrito como a "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento" (inciso II);

(iii) **princípio da necessidade**, descrito como a "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados" (inciso III);

(iv) **princípio do livre acesso**, descrito como a "garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais" (inciso IV);

(v) **princípio da qualidade dos dados**, descrito como a "garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento" (inciso V);

(vi) **princípio da transparência**, descrito como a "garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (inciso VI);

(vii) **princípio da segurança**, que exige "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão" (inciso VII);

(viii) **princípio da prevenção**, traduzido na "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (inciso VIII);

(ix) **princípio da não discriminação**, que consiste na "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos" (inciso IX);

(x) **princípio da responsabilização e prestação de contas**, que exige "demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas."

Como se pode observar, os princípios mencionados, além de evidentes conexões com a boa-fé objetiva, podem ser assim agrupados:

(i) **finalidade legítima, específica, explícita e informada** ao titular para o tratamento de dados;

(ii) **necessidade, adequação e proporcionalidade do meio** escolhido para o tratamento de dados;

(iii) **transparência e prestação de contas** sobre a forma do tratamento de dados, o que implica necessariamente a preservação da qualidade dos dados e a disponibilidade dos dados ao titular por meio do livre acesso;

(iv) **prevenção de danos e ampla responsabilização** dos agentes que tomam as decisões relativas ao tratamento de dados ou daqueles que realizam diretamente o tratamento, inclusive para efeitos de lhes imputar o ônus de demonstrar a eficácia das medidas adotadas para a prevenção de danos, bem como para deles se exigir as respectivas obrigações de segurança;

(v) **vedação de discriminações abusivas ou ilícitas.**

Embora a Lei não trate, pelo menos explicitamente, das discussões relacionadas à crescente utilização de algoritmos por agentes empresariais, é inequívoco que os princípios por ela previstos apontam no sentido da necessidade de transparência e prestação de contas sobre qualquer que seja o meio utilizado para o tratamento de dados, o que incluiria o meio algorítmico. Entretanto, a própria enunciação do princípio da transparência excetua os segredos de negócios, o que pode gerar dúvida sobre como compatibilizar os princípios em jogo.

Por outro lado, os princípios previstos no art. 6º precisam ser interpretados em conformidade com os fundamentos constantes do art. 2º, sendo certo que dificilmente os objetivos de livre desenvolvimento da personalidade e da preservação da autonomia e da cidadania podem ser alcançados sem que haja maior controle sobre o tratamento de dados via algoritmos. Da mesma maneira, sem maior transparência e *accountability* sobre os algoritmos, não se tem como assegurar a eficácia de vários dos princípios elencados pela lei, incluindo os que exigem que o meio utilizado para o tratamento de dados atenda aos requisitos da necessidade, adequação e proporcionalidade, assim como o que veda discriminações ilícitas ou abusivas.

Basta lembrar que, já nas definições constantes do seu art. 5º, a lei prevê o relatório de impacto à proteção de dados pessoais, conceituando-o como “documentação do controlador que contém a descrição dos processos de

tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (inc. XVII). Ora, sem a devida transparência sobre como os dados são utilizados, os riscos não podem ser nem suficientemente identificados nem mitigados.

Logo, mesmo a análise introdutória da Lei Geral de Proteção de Dados já permite a constatação de inúmeros desafios interpretativos, os quais serão analisados nos próximos artigos desta série.

Link: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018>

Publicado em 29/08/2018